IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

PLAINTIFFS' PROPOSAL REGARDING SECURITY PROTOCOLS FOR REVIEW OF GEMS DATABASE

Defendants continue to be unable to explain what about the GEMS databases is sensitive beyond vague references to their "structure," which Merle King has stated is the same in every state that uses GEMS and is therefore already publicly available information.[1] As Dr. Halderman states in his declaration filed with Plaintiffs' Joint Brief: "Detailed information about the operation of GEMS and the structure of the GEMS database is already part of the public record." (Doc. 441 at 440; *see also* Doc. 441 at 199 (Bernhard Decl.) and Doc. 441 at 219 (Ryan Decl.)). As a result, the GEMS databases should not be considered sensitive or confidential and should be made available immediately to Plaintiffs and their experts.

[1] *See* Doc. 441 at page 90. Merle King is the former long-time Executive Director of Center for Election Systems at KSU, where he had responsibility for the production of GEMS databases over the course of hundreds of Georgia elections.

Understanding, however, that the Court is inclined to proceed under the conditions requested by Defendants and is seeking from Plaintiffs information about whether Defendants' proposal is workable, Plaintiffs respond to explain why it is not and to present an alternative solution that would be just as secure.[2]

First, it is not reasonable or necessary to require Plaintiffs' attorneys and experts to travel hundreds of miles to Atlanta to review the GEMS databases in Defendants' facilities. This restriction would make review of the GEMS databases

[2] Plaintiffs have discussed the need to analyze two distinct kinds of data from Georgia's election system: copies of the GEMS database files for particular counties and from the Secretary of State's office ("GEMS databases") and copies of the hard drives from election management computers ("GEMS hard drives"). Plaintiffs propose that review of both these sets of information take place on secure computers in their own facilities subject to the protocol discussed below. GEMS databases are Microsoft Access files that contain the ballot layouts and other election configuration data used to program voting machines, as well as the election results from individual machines used to produce overall vote tallies. GEMS hard drives are computers are operated by the Secretary of State's office and by counties, and include GEMS servers (used for preparing voting machine programming and for tabulation), ExpressPoll data servers (used for preparing electronic poll book programming), and workstations that employees use to access these servers. The GEMS hard drives from election management computers may contain sensitive information that is necessary to keep confidential, such as personally identifying information about voters and undisclosed information about how these computers are secured. In contrast, the GEMS database files are not sensitive. GEMS database files are routinely made public in other states, and their disclosure in Georgia would not create any new security risk to the election system. The GEMS database information is widely disseminated without meaningful restrictions to 159 counties which load the databases onto thousands of memory cards and voting machines.

prohibitively expensive, logistically difficult, and unnecessarily time consuming given that review of the database will take many days and potentially weeks. Plaintiffs' representatives will need to go back to the data again and again and compare it to other data and documents to get a full picture of the issues inherent in the system. Plaintiffs' counsel and experts have experience handling highly sensitive information[3] and can be trusted to receive physical delivery of encrypted files on a CD – just as they are delivered to the counties – so that they can review the GEMS databases in their own facilities.

The State Defendants' proposed access conditions would severely impede an effective examination. The state proposes to provide a single computer with the same software environment that Georgia counties use to run GEMS. However, GEMS runs only under obsolete versions of Microsoft Windows, and an efficient analysis calls for the use of modern software. More recent operating system software is also more secure than obsolete versions, so the state's proposal would only serve to increase security risks. (Halderman Decl. at ¶ 9.)

The following protocol would allow Plaintiffs to create an environment as

[3] Curling Plaintiffs' team of attorneys includes John Carlin, former Assistant Attorney General for the U.S. Department of Justice's National Security Division and former Chief of Staff to then-FBI Director Robert S. Mueller, III. (Cross Decl. ¶¶ 2-4.)

secure as Defendants', but in Plaintiffs' own facilities[4]:

- Establish locked, secure work areas to which only Plaintiffs' attorneys and experts have access.
- Install the GEMS databases onto a limited number of air-gapped, password-protected, standalone computers ("protected PCs") that are not connected to the internet.
    - Multiple protected PCs are necessary so that Plaintiffs attorneys and experts can work in parallel.
- Plaintiffs' attorneys and experts may bring their own laptops into the secure work areas subject to the following restrictions:
    - GEMS databases would never be installed on their own laptops;
    - Laptops may be connected to the internet via an external wireless network while they are in the room, but they would not be networked to any of the protected PCs on which the GEMS databases are installed;

[4] In the alternative, Plaintiffs propose adopting the security plan developed by the Secretary of State of California for that state's 2007 "Top-to-Bottom Review" of election system security, supplemented by the procedure for extracting information outlined in the text at page 4 to 5. This plan, available at https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/source-code-security-plan.pdf, is a perfect example of the kinds of conditions a state imposes when it wants to facilitate an efficient analysis, rather than inhibit it.

  - Attorneys and experts may use removable storage media (e.g., USBs) to transfer files from the laptops to the protected PCs.

- Plaintiffs' attorneys and experts may maintain private notes that are subject to the protective order and that will never be shared with Defendants.
- Only Plaintiffs' attorneys and experts will review the full GEMS databases.
  - If the attorneys and experts identify information that can be safely extracted from the databases for review by other non-lawyer, non-expert members of Plaintiffs' teams, they will identify that information to Defendants, who will have 24 hours to raise an objection.
  - After 24 hours, if no objection is raised, Plaintiffs' attorneys and/or experts may provide the non-confidential information to the members of the team in text or Excel files. If an objection is raised, the issue will be presented to the Court for resolution, with the Defendants bearing the burden of proof.[5]

Second, the state proposes to provide only Microsoft Access and to prohibit Plaintiffs from installing any other software. Plaintiffs' experts and attorneys must

[5] Defendants bear the burden to support their confidentiality claims. *See* Plaintiffs' Joint Brief, Doc. 441, at 4 (citing cases).

be able to install appropriate software and data to protected PCs to conduct their analysis of the GEMS databases. As Defendants and their expert(s) are presumably aware, a review of the GEMS databases without the necessary tools would not allow the detection of errors, vulnerabilities, and viruses that are potentially hidden in the databases. Plaintiffs must be able to run software and use other tools in order to conduct a meaningful review of the databases. An effective examination will require additional software tools, such as specialized software to examine the low-level structure of the database, to compare multiple versions of the database, to check the data for consistency, and so on. Plaintiffs' experts will not be able to determine the full set of software tools that are necessary for their analysis until the examination is underway. With appropriate controls, software and data can be copied into the secure environment without creating any risk that confidential data will be copied out, and so the state's proposed restriction would serve only to impede the analysis. (*Id.* at ¶ 10.)

Third, Defendants' proposal seems to anticipate review only by Plaintiffs' experts. This is not feasible.[6] Both sets of Plaintiffs need a team of attorneys and support staff to review the GEMS databases given volume of data and the number of databases – there are many databases, potentially hundreds – even just at the

[6] For a detailed description of the non-expert, labor intensive work required to review the databases, *see* Plaintiffs' Joint Brief, Doc. 441 at 15-18.

state level for one election. It is not possible for two cybersecurity experts to conduct this review alone. Even if Plaintiffs had unrestricted access to the data, a complete examination of the GEMS database files is likely to take weeks of effort by a team of people. Several factors make this analysis more complicated than a routine forensic review: the size of the data; the age of the computer software involved; the specialized nature of the GEMS application; and the potential that the GEMS databases files have been altered in an attack by hostile nation-states. (*Id.* at ¶ 12.) Plaintiffs therefore propose an initial review of the system by only attorneys and experts, with the right to make the showing to this Court that the GEMS databases themselves should not be confidential once we receive it. Additionally, as noted above, Plaintiffs' attorneys and experts would have the ability to extract lines of data in isolation to send to individuals on their teams who are neither attorneys nor experts. Plaintiffs' counsel would be required to notify Defendants of the information they intended to share and Defendants would have 24 hours in which to object. This process would be expedited: the parties would seek relief from the Court if they are not able to resolve an issue within 48 hours.

Finally, Plaintiffs' attorneys and experts must be able to take and retain notes that are never shared with Defendants. Defendants' proposed restrictions would impede an effective examination by making it difficult for Plaintiffs' experts to privately confer in order to develop and test hypotheses about the data. (*Id.* at ¶ 11.) Defendants have not and cannot identify any security reason that Plaintiffs *attorneys and experts* should leave their notes with Defendants. Defendants merely wish to secure an advantage in this litigation, or perhaps they are looking for a free security analysis of their system by one of the world's leading experts; either way it would be wildly inappropriate to require Plaintiffs' experts and attorneys to share their notes with Defendants.

Respectfully submitted this 3rd day of July, 2019.

/s/ David D. Cross
David D. Cross (*pro hac vice*)
John P. Carlin (*pro hac vice*)
Jane P. Bentrott (*pro hac vice*)
Catherine L. Chapple (*pro hac vice*)
Robert W. Manoso (*pro hac vice*)
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Suite 6000
Washington, DC 20006
Telephone: (202) 887-1500
DCross@mofo.com
JCarlin@mofo.com
RManoso@mofo.com
CChapple@mofo.com
JBentrott@mofo.com

/s/ Halsey G. Knapp, Jr.
Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578
KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
HKnapp@khlawfirm.com
Sparks@khlawfirm.com

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III
Robert A. McGuire, III
Admitted Pro Hac Vice
(ECF No. 125)
ROBERT MCGUIRE LAW FIRM
113 Cherry St. #86685
Seattle, Washington 98104-2205
(253) 267-8530

Counsel for Coalition for Good Governance

/s/ Cary Ichter
Cary Ichter
Georgia Bar No. 382515
ICHTER DAVIS LLC
3340 Peachtree Road NE
Suite 1530
Atlanta, Georgia 30326
(404) 869-7600

Counsel for William Digges III,Laura Digges, Ricardo Davis and Megan Missett

/s/ David Brody
David Brody
John Powers
Lawyers' Committee for Civil Rights Under
Law
1500 K St. NW, Suite 900
Washington, DC 20005
202-662-8300
dbrody@lawyerscommittee.org
jpowers@lawyerscommittee.org

Counsel for Coalition Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

Pursuant to LR 7.1(D), I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ David D. Cross
David D. Cross

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER , ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on July 3, 2019, a copy of the foregoing **PLAINTIFFS' PROPOSAL REGARDING SECURITY PROTOCOLS FOR REVIEW OF GEMS DATABASE** was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ David D. Cross
David D. Cross